Amendments to the Specification:

Please delete the Abstract of the invention in its entirety, and add the following new Abstract:

Two devices calculate a common secret by evaluating the product of two polynomials using parameters previously distributed by a trusted third party and parameters obtained from the other party. Preferably the parties subsequently verify that the other party has generated the same secret using a zero-knowledge protocol or a commitment-based protocol. The method is particularly suitable for very low power devices such as Chip-In-Disc type devices.